

数学

清华大学 任舍予

数论结构

带余除法 \leftarrow 整除 — 同构
模

- 素数与筛法
- 整数与分解
- 整除性
 - 数论分块
 - 裴蜀定理与扩展欧几里得算法
- 数论函数
 - 积性函数
 - 莫比乌斯反演



例题

- 题意：求有多少个正整数 X ，满足 $\forall S \in [L, R] \cap \mathbb{N}$, $(S \bmod Q) \bmod X = S \bmod X$
- 数据范围： $L, R, Q \leq 10^{12}$

$$\underline{S \bmod Q} \equiv \underline{S} \pmod{X}.$$

$$x \mid \underline{S - S \bmod Q} = \underline{\left\lfloor \frac{S}{Q} \right\rfloor \cdot Q}.$$

$$\Leftrightarrow x \mid \gcd\left(\underline{\left\lfloor \frac{L}{Q} \right\rfloor \cdot Q}, \dots, \underline{\left\lfloor \frac{R}{Q} \right\rfloor \cdot Q}\right).$$

洛谷 P3951 [NOIP2017 提高组] 小凯的疑惑 / [蓝桥杯 2013 省] 买不到的数目

- 题意：求最大的正整数 x ，无法表示为 $ma + nb$ ($m, n \in \mathbb{N}, a \perp b$)
- 数据范围： $a, b \leq 10^9$

exgcd.

$$ax_0 + by_0 = 1.$$

$$x = \frac{-a + (a-1)b}{b}.$$

$$m \in [-b, -1].$$

$$x_0 \quad x_1 \quad x_2$$

$$y_0 \quad y_1 \quad y_2$$

$$+b \quad -a$$

$$a_0(x_0 + b) + b(y_0 - a) = 1.$$

$$n \in [0, a).$$

洛谷 P8338 [AHOI2022] 排列

- 题意： 对于一个长度为 n 的排列 $P = (p_1, p_2, \dots, p_n)$ 和整数 $k \geq 0$, 定义 P 的 k 次幂

$$P^{(k)} = (p_1^{(k)}, p_2^{(k)}, \dots, p_n^{(k)}),$$

该排列的第 i 项为

$$p_i^{(k)} = \begin{cases} i, & k = 0, \\ p_{p_i}^{(k-1)}, & k > 0. \end{cases}$$

容易证明任意排列的任意次幂都是一个排列。

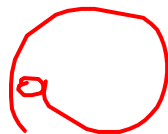
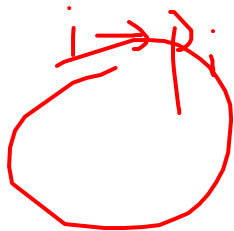
定义排列 P 的循环值 $v(P)$ 为最小的正整数 k 使得 $P^{(k+1)} = P$ 。

给出一个长度为 n 的排列 $A = (a_1, a_2, \dots, a_n)$, 对于整数 $1 \leq i, j \leq n$, 定义 $f(i, j)$: 若存在 $k \geq 0$ 使得 $a_i^{(k)} = j$, 则 $f(i, j) = 0$, 否则设排列 A_{ij} 为将排列 A 的第 i 项 a_i 和第 j 项 a_j 交换后得到的排列, 则 $f(i, j) = v(A_{ij})$ 。

求 $\sum_{i=1}^n \sum_{j=1}^n f(i, j)$ 的值。答案可能很大, 你只需要输出其对 $(10^9 + 7)$ 取模的结果。

- 数据范围： $n \leq 5 \times 10^5$

$$\sum \sum_{a_i \neq a_j} \underbrace{\text{lcm}(\{a_1, \dots, a_n\} - \{a_i, a_j\} + \{a_i + a_j\})}_{f(a_i) f(a_j)}$$



$$\text{lcm}(a_1, a_2, \dots, a_n)$$



洛谷 P9135 [THUPC 2023 初赛] 快速 LCM 变换

- 题意：
 - 给定正整数序列 $\{r_n\}$, 选择正整数 $1 \leq i < j \leq n$, 删除 r_i, r_j , 加入 $r_i + r_j$
 - 求所有方案的序列中所有数的 lcm 之和
- 数据范围： $n \leq 5 \times 10^5$, $r_i \leq 10^6$



数论定理

- 费马小定理 & 欧拉定理
- 线性同余方程组
 - 中国剩余定理
 - 线性同余方程的合并/exCRT

$$p, a \neq 0 \pmod{p}.$$

$$a^{p-1} \equiv 1.$$

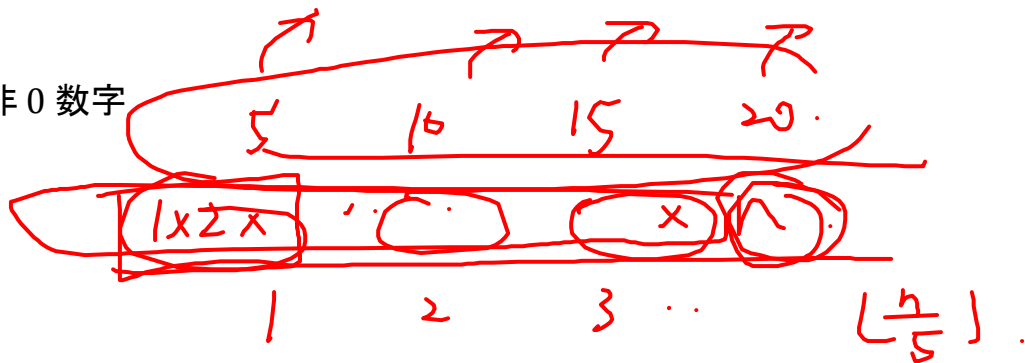
$$m. (a, m) = 1 \quad a^{\phi(m)} = 1.$$



例题

- 题意：求 $n!$ 末尾 0 的个数与最后一位非 0 数字
- 数据范围： $n \leq 10^{18}$

$n!$ 5 的个数.



$$k = \text{ans1}_n = \left\lfloor \frac{n}{5} \right\rfloor + \text{ans1}_{\left\lfloor \frac{n}{5} \right\rfloor}$$

$$\frac{n!}{5^k} \pmod{10}$$

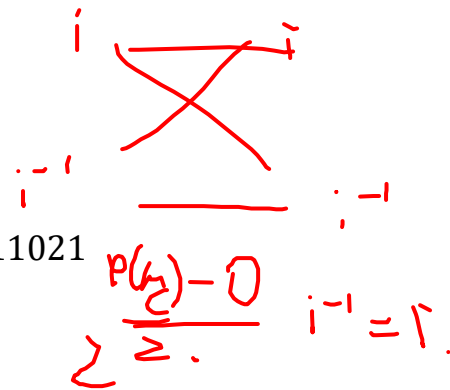
$$\frac{n!}{5^k} \pmod{5}$$

$$\text{ans2}_n = (-1)^{\left\lfloor \frac{n}{5} \right\rfloor} \cdot (n/5)! \cdot \text{ans2}_{\left\lfloor \frac{n}{5} \right\rfloor} \pmod{5}$$

LOJ #563. 「LibreOJ Round #10」 Snakes 的 Naïve Graph

- 题意：

- 给定 $2m - 2$ 个点的二分图 $G(m)$
- 左侧第 i 个点和右侧第 j 个点有连边当且仅当 $i = j \vee ij \equiv 1 \pmod{m}$
- 设 $f(m)$ 表示 $G(m)$ 的本质不同的最大匹配的个数，求 $(f(1) \sim f(n)) \bmod 311021$
- 数据范围： $n \leq 10^7$



$$x^2 - 1 \equiv 0 \pmod{p^k}$$

$$p^k \mid (x-1)(x+1)$$

$$\left\{ \begin{array}{l} p^k \mid x-1 \\ p^k \mid x+1 \end{array} \right.$$

$p > 2$.

$$x^2 \equiv 1 \pmod{m}$$

$$x^2 \equiv 1 \pmod{p_i^{\alpha_i}}$$

$$\prod_{i=1}^k g(p_i^{\alpha_i})$$

$$x = 2^{k-1} + 1 \quad (p \geq 2)$$

$$x = 1$$

$$g(p^k)$$

$$g(2) \quad g(4)$$

$$g(2^k) \quad k \geq 5$$

数列

- 递推与通项
- 模意义下数列的循环节

$$a_n = p a_{n-1} + q \quad \hookrightarrow$$

$$\underline{a_n - t = p(a_{n-1} - t)}$$

$$a_n = p^n(a_0 - t) + t$$

$$a_n = p a_{n-1} + q a_{n-2}$$

$$\underline{a_n - t a_{n-1}} = \frac{(p-t) a_{n-1} + q a_{n-2}}{(p-t) \left(a_{n-1} + \frac{q}{p-t} a_{n-2} \right)}$$

$= -t$

洛谷 P3263 [JLOI2015] 有意义的字符串

- 题意：求 $\left\lfloor \left(\frac{b+\sqrt{d}}{2} \right)^n \right\rfloor \bmod 7528443412579576937$

- 数据范围： $n \leq 10^{18}$, $0 < b^2 \leq d < (b+1)^2 \leq 10^{18}$, $b \equiv 1 \pmod{2}$, $d \equiv 1 \pmod{4}$.

$$\left(\frac{b+\sqrt{d}}{2} \right)^n + \left(\frac{b-\sqrt{d}}{2} \right)^n$$

$$\underline{a_0 = 2} \quad \underline{a_1 = b} \quad \underline{P, L:}$$

线性代数

- 矩阵
- 高斯消元
- 线性方程组
- 矩阵求逆
- 行列式
- 线性基

